UNITED STATES DISTRICT COURT

DISTRICT OF NEVADA

UNITED STATES OF AMERICA, Plaintiff, v. MARIO CASTRO, Defendant.	Case No.: 2:19-cr-00295-GMN-NJK **REPORT AND RECOMMENDATION** [Docket No. 254]

This matter was referred to the undersigned Magistrate Judge on Defendant Mario Castro's motion to suppress evidence. Docket No. 254. The Court has considered Defendant's motion, the United States' response, and Defendant's reply. Docket Nos. 254, 257 (corrected image), 270, 275.

I. BACKGROUND

On February 15, 2018, United States Magistrate Judge Peggy A. Leen issued two search warrants – one for Defendant's residence, and one for his office – both supported by the same 66-page affidavit, plus its attachments. *See* Docket Nos. 257-1, 270-1.[1] For each property, the warrant authorized the search of the entire property, including all visible structures and any locked containers, computers, cellular phones, storage media, and vehicles.[2] Docket Nos. 257-1 at 77-81, 270-1 at 6, 21. The warrants authorized the seizure of all records and information constituting fruits, contraband, evidence, and instrumentalities of violations of mail fraud, wire fraud,

[1] Both parties rely upon the affidavit in support of the search warrants and attachments thereto for the facts. *See, e.g.*, Docket Nos. 257 at 2, 270 at 3. The Court therefore derives its factual background from the same documents. *See* Docket No. 257-1.

[2] The warrant for Defendant's business also authorized the search of any safe located on the premises. Docket Nos. 257-1 at 79, 270-1 at 21.

conspiracy to commit mail fraud, and money laundering that related to mass-mailed consumer fraud schemes. Docket Nos. 257-1 at 86-89, 270-1 at 8-11, 24-27. The warrants authorize a non-exhaustive list of types of records or information that could fit under this categorization, including records related to persons and entities working in concert with the alleged scheme; customer databases or lists; draft and final solicitations; draft and final collection letters; third party legal notices; mailing records; correspondence; computer records; and computer equipment. *Id.* The warrants also set forth a protocol for how electronic data would be forensically analyzed. Docket Nos. 257-1 at 90-94, 270-1 at 12-16, 28-32.

The affidavit in support of both warrants submits that, beginning in at least 2004, a mail fraud scheme was initiated which involved mass mailing fraudulent solicitations though the U.S. mail. *See* Docket No. 257-1 at 6-7, 33.[3] The affidavit states that the solicitations sought payments or processing fees for large cash prizes or services which were never paid out. *Id.* at 7. The affidavit further states that millions of dollars were collected through this scheme. *Id.* The affidavit lays out the components of how the scheme worked, including how individuals operated within the scheme and the businesses used to print or send out the fraudulent mailings. *Id.* at 7-34. The affidavit states that participants in the scheme would print and mail the solicitations and would use other agents or services to facilitate the mailing and to rent private mailboxes to receive the returns to be distributed among the participants. *Id.* at 7-9.

The affidavit states that bank accounts were created and used to transfer money between the various members of the scheme. *Id.* at 38-54. The affidavit includes locations identified by IP addresses from which those bank accounts were accessed. *Id.* at 38-54. The affidavit states that 25 bank accounts were connected to various targets of the investigation into the scheme, and that Defendant was the primary account holder for six of those accounts. *Id.* at 34-35. The affidavit further sets forth the ways in which Defendant and the other participants in the scheme used email, computers, and cell phones to conduct the scheme. *Id.* at 63-67. These included using electronic

[3] The affidavit includes information obtained in an interview that one target of the investigation received victim mail from a commercial mail receiving agency box in 2004. Docket No. 257-1 at 33. The same interview provided information that another target who was allegedly not in the mailing business attended a direct mailing trade show in 2000. *Id.*

devices to prepare and share the solicitations at issue; email and text correspondence with other alleged members of the scheme and the commercial mail receiving agency locations; databases detailing solicitations that were sent out and money received in response to solicitations; calendars for mailings; and further financial records detailing how much money the scheme had acquired. *Id.*

The affidavit states that Defendant was a member of the overall fraud scheme and used his business in furtherance of the scheme. *Id.* at 14. The affiant alleges that Defendant was the president of Digital Express and Pi Printing, which were both part of the overall fraudulent syndicate. *Id.* Specifically, the affidavit states that they offered printing services for the operation. *Id.* The affidavit also states that Defendant opened mailboxes in New York and Arkansas in the names of Monies Securities and Assets Unlimited for the processing fees to be collected and forwarded to another member of the overall fraud scheme. *Id.* at 32-33. The affidavit states that nine other boxes were opened by other targets of the investigation in the names of companies with bank accounts that were accessed from Defendant's home and workplace. *See id.*

The affidavit further states that Defendant or another person used the Internet at both Defendant's house and workplace to log on to the online bank accounts associated with the fraudulent scheme. *Id.* at 48-51. Particularly, the affidavit references Bank of America records showing Cox IP addresses assigned to both Defendant's house and workplace as being used to access bank accounts associated with Digital Express, Inc., Pi Printing Corp, and Pi Printing Corp d/b/a Assets Unlimited. *Id.* The affidavit states that the records also show that the Cox IP address associated with Defendant's workplace was used for access accounts for Advanced Allocation Systems Inc. d/b/a Pacific Disbursement Reporting, Marketing Image Direct Inc. d/b/a Price Awards, and Pacific Allocations Systems Inc. *Id.* at 50-51. The affidavit states that these accounts were accessed numerous times in 2016 and 2017. *Id.* at 48-51. According to the affidavit, Defendant's house was the primary address for four of the bank accounts associated with the scheme. *Id.* at 48-49.

The affidavit further includes information about phone records showing over 1000 distinct communications, by telephone call and text message, involving numbers registered to Defendant.

Id. at 49, 51. The affidavit states that these numbers were registered to Defendant for his home and his business and that the communications were with various other members of the scheme. *Id.*

The affidavit also includes a list of the property to be seized and protocols governing the searches of electronic devices. *Id.* at 86-94. Judge Leen reviewed and approved the specific property to be seized, including records and information relating to the alleged mail fraud and money laundering schemes at the center of the instant case; customer databases and lists; draft and complete solicitations; draft and final collection letters; legal notices from third parties; invoices, business records, and financial records related to payments received from consumers and from other members or entities associated with the scheme; fulfillment items related to the solicitations; correspondence related to the overall scheme; and shipping and mailing records. *Id.* at 86-87. The warrants also authorize the seizure of evidence related to who controlled electronic devices seized pursuant to each warrant; evidence of software that might corrupt or hide files; information about the IP addresses associated with the devices; and passwords or encryption keys needed to access the information and data on the devices. *Id.* at 88-89. The property to be seized had to be related to the offenses set forth in the affidavit and within the relevant time period from December 1, 2004, through the date of the warrants' executions. *Id.* at 86.

In February 2018, United States Postal Inspectors executed the search warrants on Defendant's home and business. Docket No. 270 at 3. On November 12, 2019, a grand jury sitting in Las Vegas, Nevada issued an indictment charging Defendant with one count of conspiracy to commit mail fraud, in violation of 18 U.S.C. § 1349, and twelve counts of mail fraud, in violation of 18 U.S.C. § 1341. Docket No. 1. Defendant was arrested and appeared for his initial appearance on November 13, 2019. Docket Nos. 17, 32. Defendant now asks the Court to suppress all evidence seized pursuant to these two warrants. Docket No. 254.

II. ANALYSIS

A. Evidentiary Hearing

The United States Court of Appeals for the Ninth Circuit has held that an evidentiary hearing on a motion to suppress need only be held if the moving papers allege facts with sufficient definiteness, clarity, and specificity to enable the court to conclude that contested issues of material

fact exist. *United States v. Howell*, 231 F.3d 615, 620 (9th Cir. 2000) (*citing United States v. Walczak*, 783 F.2d 852, 857 (9th Cir. 1986); *United States v. Harris*, 914 F.2d 927, 933 (7th Cir. 1990); *United States v. Irwin*, 613 F.2d 1182, 1187 (9th Cir. 1980); *United States v. Carrion*, 463 F.2d 704, 706 (9th Cir. 1972).

"A hearing will not be held on a defendant's pre-trial motion to suppress merely because a defendant wants one. Rather, the defendant must demonstrate that a 'significant disputed factual issue' exists such that a hearing is required." *Howell*, 231 F.3d at 621 (*citing Harris*, 914 F.2d at 933). The determination of whether an evidentiary hearing is appropriate rests in the reasoned discretion of the district court. *United States v. Santora*, 600 F.2d 1317, 1320 (9th Cir.), *amended by* 609 F.2d 433 (1979). In the instant case, Defendant requested an evidentiary hearing; however, both parties relied upon the same discovery in presenting the facts and Defendant's arguments stem from the face of the warrant language. The Court concludes that no contested issues of fact exist that require an evidentiary hearing in this matter, and the Court will therefore decide the motion on the moving and responsive papers, including the exhibits submitted with the papers.

B. Motion to Suppress

Defendant asks the Court to suppress any evidence the United States obtained as a result of the searches of his house and his business. Docket Nos. 254, 257. In support of his motion, Defendant submits that the warrants were fatally defective. Specifically, Defendant submits that the warrants lacked specificity and were overbroad because the affidavit in support of the warrants failed to establish probable cause to search for or seize any materials or records prior to 2014, but nonetheless authorized the search for items related to a time period beginning on December 1, 2004. Docket No. 257 at 6-7. Defendant further submits that the affidavit and its attachments did not provide any objective standards for the executing officers to minimize exposure of electronic content that was not responsive to the warrants, as the electronic search protocol was overbroad. *Id.* at 8-9, 11-13. Further, Defendant submits that the warrants lacked particularity as they only

listed broad, generic categories of items sought. *Id.* at 9-11.[4] Defendant therefore asks the Court to suppress all evidence seized in connection with the search warrant. *Id.* at 13.

In response, the United States submits that the search warrants properly met the standards for particularity, specificity, and breadth. Docket No. 270 at. The United States submits that the affidavit in support of the warrants established probable cause that the underlying fraudulent scheme began in 2004 and was ongoing and that the time period was not overbroad as other communications or evidence related to the scheme predating Defendant's involvement could be found. *Id.* at 5-7. The United States further submits that the warrants were particular, as they contained proper limiting information and guidance, and that the included categories of items and evidence were not overly general. *Id.* at 5-6, 8-9. Moreover, the United States submits that the electronic search protocols to which Defendant objects were not mandatory as their inclusion was not legally required; therefore, they could not invalidate the underlying warrants. *Id.* at 9-11. Finally, the United States submits that any error the Court might find in the underlying warrants would not require suppression of the evidence seized because the officers executing the warrant acted in good faith. *Id.* at 12-13.

In reply, Defendant submits that the warrants lacked particularity and were overbroad because they authorized a search for a time period that was a decade longer than Defendant's alleged involvement in the underlying scheme. Docket No. 275 at 2-5. Defendant also submits that the good faith exception does not remedy the underlying issue because the defects in the warrants are obvious from the face of the documents. *Id.* at 5-10. Defendant asks the Court to suppress all evidence and the fruits of the evidence collected pursuant to these two warrants. *Id.* at 10.

. . . .

. . . .

[4] In his reply, Defendant raises for the first time that suppression is necessary because the agents executing the warrant ignored the language of the electronic search protocol. Docket No. 275 at 9. The Court will not consider arguments raised for the first time in a reply brief. *See United States v. Gianelli*, 543 F.3d 1178, 1184 n.6 (9th Cir. 2008) (arguments raised for the first time on reply are generally considered waived); *Zamani v. Carnes*, 491 F.3d 990, 997 (9th Cir. 2007) ("The district court need not consider arguments raised for the first time in a reply brief.").

1. Probable Cause

The Fourth Amendment secures "the right of the people to be secure in their persons, houses, papers, and effects against unreasonable searches and seizures." U.S. Const. amend. IV. Evidence obtained in violation of the Fourth Amendment, and evidence derived from it may be suppressed as the "fruit of the poisonous tree." *Wong Sun v. United States*, 371 U.S. 471, 484-87 (1963); *United States v. Lundin*, 817 F.3d 1151, 1157 (9th Cir. 2016).

The Fourth Amendment's Warrant Clause provides that a warrant may be issued only "upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized." U.S. Const. amend. IV. This language imposes three requirements. *Dalia v. United States*, 441 U.S. 238, 255 (1979). A valid search warrant must be: (1) issued by a neutral and detached judge; (2) supported by probable cause to believe the evidence sought will aid in a particular apprehension or conviction for a particular offense; and (3) describe the things to be seized and the place to be searched with particularity. *United States v. Artis*, 919 F.3d 1123, 1129 (9th Cir. 2019) (citing *Dalia*, 441 U.S. at 255).

Probable cause exists if there is a "fair probability that contraband or evidence of a crime will be found in a particular place." *Illinois v. Gates*, 462 U.S. 213, 238 (1983). Probable cause is "a fluid concept turning on the assessment of probabilities and the particular factual context not readily, or even usefully, reduced to a neat set of legal rules," and its existence must be determined by an analysis of the totality of the circumstances surrounding the intrusion. *Id*. at 232. Determining whether probable cause exists "turn[s] on the assessment of probabilities in particular factual contexts." *Id*. The concept does not deal with hard certainties, but with probabilities. *Id*. at 241; *see also Brinegar v. United States*, 338 U.S. 160, 175 (1949) (Probable cause deals with "probabilities" which are not technical, but factual and practical considerations of everyday life on which reasonable and prudent people, not legal technicians act). The United States Supreme Court has repeatedly emphasized that the probable cause standard is a "practical, non-technical conception." *Brinegar*, 338 U.S. at 175.

The probable cause standard for a search warrant is whether, based on common sense considerations, there was "a fair probability that contraband or evidence of a crime [would] be

found in a particular place." *United States v. DeLeon*, 979 F.2d 761, 764 (9th Cir.1992) (citing *Gates*, 462 U.S. at 238). The magistrate judge need not determine "that the evidence is more likely than not to be found where the search takes place. . . . The magistrate [judge] need only conclude that it would be reasonable to seek the evidence in the place indicated in the affidavit." *United States v. Ocampo*, 937 F.2d 485, 490 (9th Cir.1991) (citation and internal quotation marks omitted). Neither certainty nor a preponderance of the evidence is required. *United States v. Kelley*, 482 F.3d 1047, 1050–51 (9th Cir. 2007) (citing *Gates*, 462 U.S. at 246 (1983) and *United States v. Gourde*, 440 F.3d 1065, 1069 (9th Cir. 2006) (*en banc*)).

The *Gates* decision made it clear that a magistrate judge's decision regarding probable cause should be given great deference. The duty of a reviewing court is to insure that the issuing judge had a substantial basis for concluding that probable cause existed. The Supreme Court has declined to articulate a "neat set of legal rules" for evaluating probable cause, *Gates*, 462 U.S. at 232, and instead has instructed magistrate judges to determine probable cause by considering the "totality-of-the-circumstances," *Gates*, 462 U.S. at 230. In issuing a search warrant, the magistrate judge simply must determine whether there is a "fair probability" that evidence of a crime will be found. *Id*., 462 U.S. at 238, 246. A reviewing court is required to examine all circumstances set forth in the affidavit, and in doubtful cases, to give preference to the validity of the warrant. *United States v. Peacock*, 761 F.2d 1313, 1315 (9th Cir.), cert. denied, 474 U.S. 847 (1985). A judge's determination that an affidavit provided probable cause to issue a warrant "will be upheld unless clearly erroneous." *United States v. Alvarez*, 358 F.3d 1194, 1203 (9th Cir. 2004).

It is well recognized that law enforcement officers can rely on their own experience and the experience and information of other law enforcement officers in establishing probable cause. *United States v. Butler*, 74 F.3d 916 (9th Cir. 1996). Similarly, "a magistrate [judge] may rely on the conclusion of experienced law enforcement officers regarding where evidence of a crime is likely to be found." *United States v. Fannin*, 817 F.2d 1379, 1381 (9th Cir. 1987). *See also United States v. Ayers*, 924 F.2d 1468, 1479 (9th Cir. 1991) ("in weighing the evidence supporting a request for a search warrant, a magistrate [judge] may rely on the conclusions of experienced law enforcement officers regarding where evidence of a crime is likely to be found"). An officer need

not include all the information in his possession to obtain a search warrant. An affidavit need only show facts adequate to support the finding of probable cause. *United States v. Johns*, 948 F.2d 599, 605 (9th Cir. 1991).

Reviewing the affidavit as a whole, applying the totality of the circumstances test, and showing the issuing judge great deference as the Supreme Court requires, the Court concludes that the issuing judge had a substantial basis for finding that probable cause existed to issue both the warrant for Defendant's house and for his workplace. The extensive affidavit sets forth detailed connections between the alleged fraud scheme and Defendant, his home, and his workplace. The affiant sets forth his experience in other investigations of similar fraud schemes; his understanding of the mechanism of how the alleged scheme at issue in the instant case functioned; third-party consumer mail agency, Internet, and phone connections to Defendant and both his residence and his workplace;[5] his review of solicitations that had been sent as part of the scheme, including one from a company that Defendant was in charge of; information supporting a representation that various kinds of technology, including phones and computers, were used to further the scheme; and previously collected evidence supporting a belief that the scheme began at least as early as 2004. In looking at the totality of the circumstances, the Court therefore finds that a fair probability existed that evidence of a crime would be discovered both at Defendant's home and at Defendant's workplace, as specified in the affidavit and that the search warrants are therefore valid. *See Gates*, 46 U.S. at 230-31.

---

[5] The affidavit states that Bank of America records show Cox IP addresses assigned to both Defendant's house and workplace being used to access bank accounts associated with Digital Express, Inc., Pi Printing Corp, and Pi Printing Corp d/b/a Assets Unlimited. Docket No. 257-1 at 48-51. The records also show that the Cox IP address associated with Defendant's workplace was used to access accounts for Advanced Allocation Systems Inc. d/b/a Pacific Disbursement Reporting, Marketing Image Direct Inc. d/b/a Price Awards, and Pacific Allocations Systems Inc. *Id.* at 50-51. These accounts were accessed numerous times over 2016 and 2017. *Id.* at 48-51. The affidavit also includes information about phone records showing over 1000 distinct communications by telephone call or text between numbers registered to Defendant, both at his home number and for his business Digital Express, and various other target members of the scheme. *Id.* at 49, 51. The affidavit further includes information that Defendant was the person who opened two commercial mail receiving agency boxes, one in New York and one in Arkansas, both of which forwarded all their mail to another member of the alleged scheme. *Id.* at 32-33. Nine other boxes were opened by other targets of the investigation in the names of companies with bank accounts that were accessed from Defendant's home and workplace. *See id.*

The Court finds that Defendant's argument about the temporal limitation in the warrants is without merit. Judge Leen found that probable cause supported the alleged fraudulent scheme beginning in 2004 and that Defendant was a member of the scheme. The relevant criminal activity underlying the probable cause was the fraud scheme at large, not exclusively Defendant's role in the scheme. Time periods are generally not *de facto* requirements for a warrant to be issued, although they can be required for the search of electronic data to protect from overbreadth and provide a limiting function. *See United States v. Lofstead*, 2021 U.S. Dist. LEXIS 224735, at *20-21 (D. Nev. Nov. 22, 2021). Here, the warrants at issue contain a temporal limitation based on the fraudulent scheme set forth in the affidavit. Defendant has proffered no reasons why the warrants had to specifically be limited to his alleged personal involvement in the scheme for a nexus to exist or why the warrants might not be valid on the basis that other relevant evidence predating Defendant's alleged personal involvement in the scheme existed at the two locations, such as old draft solicitations or databases including information from solicitations mailed prior to his involvement. The Court finds that Judge Leen's probable cause determination was supported by the affidavit and further finds that Defendant has provided no compelling or justifiable reasons as to why the temporal limitation is inappropriate or undermines that probable cause finding.[6]

2. Specificity

Search warrants must be specific. *United States v. Hill*, 459 F.3d 966, 973 (9th Cir. 2006). "Specificity has two aspects: particularity and breadth. Particularity is the requirement that the warrant must clearly state what is sought. Breadth deals with the requirement that the scope of the warrant must be limited by the probable cause on which the warrant is based." *Id.* (citing *United States v. Towne*, 997 F.2d 537, 544 (9th Cir. 1993)).

The particularity requirement exists to prevent general searches. *Maryland v. Garrison*, 480 U.S. 79, 84 (1987). The particularity requirement functionally limits the authority to search

[6] Suppression would not be warranted even if the Court found that a lack of a temporal limit rendered the warrant invalid. The Ninth Circuit applies "the doctrine of severance which allows [the Court] to strike from a warrant those portions that are invalid and preserve those portions that satisfy the Fourth Amendment. Only those articles seized pursuant to the invalid portions need to be suppressed." *Flores*, 802 F.3d 1028, 1045 (9th Cir. 2015) (quoting *United States v. Gomez-Soto*, 723 F.2d 649, 654 (9th Cir. 1984)).

by the probable cause that supports the search, ensuring that the search will be carefully tailored to its justifications instead of a wide-ranging exploratory search such as those specifically prohibited by the Fourth Amendment. *Id.*; *see also In re Search of Google Email Accounts identified in Attachment A*, 92 F.Supp.3d 944, 950 (D. Alaska 2015) (citing *Payton v. New York*, 445 U.S. 573, 584 n.21 (1980)). The need to prevent general exploratory searching of a person's belongings is particularly of concern in document searches because, unlike other objects, document searched tend to involve broad disclosures of the intimacies of private lives, transactions, and thoughts. *United States v. Washington*, 797 F.2d 1461, 1468 (9th Cir. 1986). However, the Ninth Circuit has often recognized a legitimate law enforcement need to collect large quantities of data and search through it carefully for concealed or disguised pieces of evidence. *See, e.g.*, *Hill*, 459 F.3d at 973.

To satisfy the particularity requirement, the "description must be specific enough to enable the person conducting the search reasonably to identify the things authorized to be seized." *United States v. Fries*, 781 F.3d 1137, 1151 (9th Cir. 2015) (quoting *United States v. Smith*, 424 F.3d 992, 1004 (9th Cir. 2005)). In determining whether a warrant is sufficiently particular, the Ninth Circuit considers one or more of the following factors: (1) whether probable cause exists to seize all items of a particular type described in the warrant; (2) whether the warrant sets out objective standards by which the executing officers can differentiate items subject to seizure form those which are not; and (3) whether the government was able to describe the items more particularly in light of the information available to it at the time the warrant was issued. *See, e.g.*, *United States v. Mann*, 389 F.3d 869, 878 (9th Cir. 2004) (quoting *United States v. Spilotro*, 800 F.2d 959, 963 (1986)).

A warrant's description of items needs to be only "reasonably specific, rather than elaborately detailed." *Hill*, 459 F.3d at 973 (citing *United States v. Storage Spaces Designated Nos. 8 & 49*, 777 F.2d 1363, 1368 (9th Cir. 1985)). A warrant with generic categories of items will not be necessarily invalidated "if a more precise description of the items . . . is not possible." *Id.* The level of specificity required "varies depending on the circumstances of the case and the type of items involved. *Id.*; *see also Spilotro*, 800 F.2d at 963-65 (noting that warrants that

"describe[e] the criminal activit[y] . . . rather than simply referring to the statute believed to have been violated" provide more substantive guidance which can satisfy the particularity requirement).

The breadth requirement functions to "limit the scope of the search warrant by the probable cause on which the warrant is based." *Fries*, 781 F.3d at 1151 (quoting *Smith*, 424 F.3d at 1004); *see also Hill*, 459 F.3d at 973. The overbreadth analysis asks the Court to assess a tailoring question: "does the proposed warrant limit the government's search to the specific places that must be inspected to confirm or dispel the suspicion that gave rise to probable cause?" *In re Search of Google Email*, 92 F.Supp.3d at 950 (citing *Garrison*, 480 U.S. at 84)).

Defendant submits that the warrants lack particularity and are overbroad. The Court finds that Defendant's particularity arguments are without merit. Probable cause exists to seize all items of the categories listed in the warrants, as the property to be seized set forth in Attachment B lists a variety of kinds of documents and records that were tied specifically to the underlying scheme set forth in the affidavit. The types of documents and records being sought were particular to the operation of the fraud scheme.

The affidavit in support of the warrants sets forth objective standards by which executing officers could differentiate items subject to seizure from those which were not. The Ninth Circuit "consider[s] an affidavit to be part of a warrant, and therefore potentially curative of any defects, only if (1) the warrant expressly incorporated the affidavit by reference and (2) the affidavit either is attached physically to the warrant or at least accompanies the warrant while agents execute the search." *United States v. SDI Future Health, Inc.*, 568 F.3d 684, 699 (9th Cir. 2009) (quoting *United States v. Kow*, 58 F.3d 423, 429 n.3 (9th Cir. 1995)).

Here, the warrants expressly incorporate the affidavit and its attachments, *see* Docket No. 257-1 at 86; Docket No. 270-1 at 3, 8, 19, 24, and the United States submits that every agent executing the warrant read the affidavit. Docket No. 270 at 3. Attachment B includes specific limiting language to guide the search, including the time frame of the fraud scheme, the underlying subject matter of the fraud scheme including suspected participating individuals and entities, and a list of the kinds of records and documentation that might be found connected to the scheme set forth in the affidavit. Docket Nos. 257-1 at 86-89; 270-1 at 8-11, 24-27. A nexus between the

alleged fraud scheme being investigated and the kinds of documentation and records being sought exists from the allegations set forth in the affidavit about the bank accounts, phone correspondence, and information about how technology was used to perpetrate the scheme. Accordingly, the Court finds that the warrants are sufficiently particular.

The Court further finds that the warrants are not overbroad. The warrants are limited to searching for documentation and items that either support or dispel the fraud scheme underlying the investigation. The affidavit sets forth prior investigative efforts that the affiant undertook which lead him to believe that Defendant was involved in at least some activities related to the scheme at both his home and his workplace. The warrants are properly tailored to Defendant's home and workplace to particularly search for evidence supporting or dispelling whether Defendant was involved in the scheme. The warrants allow a search for no more evidence than necessary to either confirm or dispel that belief. Further, courts routinely approve searches for identity information related to control over records or documents and the information supporting probable cause directly link Defendant's electronic devices to the scheme's activity. *See, e.g.*, *United States v. Turner*, 2022 WL 195083, 2022 U.S. Dist. LEXIS 11183, at * 5, 12-18 (D. Nev. Jan. 21, 2022) (finding a warrant valid which sought to seek basic user identity information related to electronic data). Accordingly, the Court finds that the warrants are not overbroad.

3. Electronic Search Protocols

The Court finds that Defendant's arguments about the electronic search protocol are unavailing. The Ninth Circuit has repeatedly acknowledged that over-seizing "is an accepted reality in electronic searching because there is no way to be sure exactly what an electronic file contains without somehow examining its content." *United States v. Flores*, 802 F.3d 1028, 1044-45 (9th Cir. 2015) (quoting *United States v. Comprehensive Drug Testing, Inc.*, 621 F.3d 1162, 1177 (9th Cir. 2010)). Data that used to be kept physically is now routinely kept electronically, and there can be challenges in retrieving electronically stored information. *Comprehensive Drug Testing, Inc.*, 621 F.3d at 1175. Additionally, courts are hesitant to narrow search protocols for digital information because digital files are easy to disguise or rename, and evidence could escape discovery. *United States v. Adjani*, 452 F.3d 1140, 1150 (9th Cir. 2006). While courts are not

required to impose protocols, they can require them for search warrants and must balance the government's interest in law enforcement and the right of individuals to be free from unreasonable searches and seizures of electronic data on a case-by-case basis. *United States v. Schesso*, 730 F.3d 1040, 1050 (9th Cir. 2013). Generally, a warrant to search electronic data will sufficiently protect against overbreadth if the warrant (1) specifies the particular crime for which evidence is sought; (2) prohibits the retention of unresponsive information under a plain-view doctrine; and (3) protects third party rights by segregating unresponsive information. *Flores*, 802 F.3d at 1045.

The Court finds that the electronic search protocol at issue here meets constitutional muster. The affidavit sets forth the offenses of mail fraud, wire fraud, money laundering, and conspiracy as the offenses for which evidence is being sought. Docket No. 257-1 at 9-11. The affidavit provides an extensive overview of the scheme at the heart of the instant case and the intricacies of its operations. The affidavit establishes the affiant's background working on computers and other kinds of technology that might contain electronic data; the grounds for onsite duplication of data for offsite review to maintain only the warrant responsive data; and the ways in which the individuals described in the affidavit used various kinds of technology in furtherance of their overall fraud scheme. *Id.* at 55-65. The affidavit further establishes a fair probability that the fraud scheme was facilitated by the targets of the warrant using a variety of electronic forms of communications. *Id.* at 63-67.

While the protocol is not mandatory, it meets the requirements set forth by Ninth Circuit precedent. The protocol outlines the crimes for which information is being sought by incorporating the attachment with information to be seized which sets forth the five offenses. The protocol has a provision providing that unresponsive plain view information will not be retained, but mandating an application for a supplemental warrant to seize such information. The protocol also contains procedures setting forth how the responsive and unresponsive information will be separated and stored to ensure proper protection of privacy rights. Moreover, the protocol limits the data seized to the time period relevant to the probable cause finding; that is, 2004 through the date the warrants were executed. Given that the protocol satisfies the Ninth Circuit's requirements, its inclusion

does not invalidate the warrants. Accordingly, suppression is not warranted due to the electronic search protocol.

C. RECOMMENDATION

Based on the foregoing and good cause appearing therefore, **IT IS RECOMMENDED** that Defendant's motion to suppress, Docket No. 254, be **DENIED.**

IT IS SO ORDERED.

DATED: March 30, 2022.

NANCY J. KOPPE
UNITED STATES MAGISTRATE JUDGE

NOTICE

This report and recommendation is submitted to the United States District Judge assigned to this case pursuant to 28 U.S.C. § 636(b)(1). A party who objects to this report and recommendation must file a written objection supported by points and authorities within fourteen days of being served with this report and recommendation. Local Rule IB 3-2(a). Failure to file a timely objection may waive the right to appeal the district court's order. *Martinez v. Ylst*, 951 F.2d 1153, 1157 (9th Cir. 1991).